Chapter 14
Behavioral Security:
Investigating the Attitude of Nursing Students Toward Security Concepts and Practices

Stelios Daskalakis
National and Kapodistrian University of Athens, Greece

Maria Katharaki
National and Kapodistrian University of Athens, Greece

Joseph Liaskos
National and Kapodistrian University of Athens, Greece

John Mantas
National and Kapodistrian University of Athens, Greece

ABSTRACT

Information and computer security are gaining continuous attention in the context of modern organizations across all domains of human activities. Emphasizing on behavioral factors toward the applicability of security measures and practices is an area under research, aiming to look beyond the strict technical peculiarities and investigate human attitudes in regards to security consciousness and familiarity. The aim of this chapter is to shed light on those aspects in relation with healthcare, by empirically assessing the intention of undergraduate nursing students to apply security concepts and practices. A research theoretical framework is proposed based on an empirical synthesis of constructs adopted from well established theories as the Health Belief Model and the Protection Motivation Theory along with a variety of previous research works. The model is then empirically tested and validated against a sample of 149 undergraduate nursing students. Data analysis was performed using partial least squares. The research findings highlighted the significant effects of perceived benefits, general security orientation and self-efficacy to behavioral intention along with the positive effect of general controllability to self-efficacy of nursing students in applying security concepts and practices, whereas a series of other constructs did not prove to be significant. The study outcomes contribute to further observations related with behavioral

DOI: 10.4018/978-1-61692-895-7.ch014

security. Despite the fact that the current empirical study was conducted under a specific context and settings, implications are discussed, regarding the security readiness of nursing students prior their engagement to a real healthcare environment.

INTRODUCTION

In today's knowledge-based economy, Information and Communication Technology (ICT) is no longer an optional 'add-on' or a 'nice to have' supporting tool for existing organizational practices. Instead, it tends to be a necessity for every organization that struggles to remain competitive in its corresponding marketplace and expand its scope of business influence. The same necessity applies not only to business-oriented organizations, but to every institutional entity that provides services of any kind. This evolution of ICT in organizations acts as a framework for promoting the quality of services provided, and consequently achieving operational excellence.

Despite the obvious direct and indirect advantages, there are also several security related concerns in current information-oriented organizations (Herath & Rao, 2009). Ensuring information integrity requires continuous monitoring and the protection of information assets is a first class priority within modern organizational structures. Information Systems (IS) are playing a key role in information security, as they are the actual medium for data handling (Ng & Xu, 2007). With regards to IS software applications, they are mainly classified either as "*preventive/protective*" or "*beneficial*", depending on their operational use (Chenoweth, Minch, & Gattiker, 2009; Dinev & Hu, 2005). Typical examples of beneficial applications include word processing, spreadsheets and other similar software. On the contrary, preventive software includes a diversity of applications that provide protection over certain types of threats (Chenoweth et al., 2009; Dinev & Hu, 2005). Typical examples of such software include firewalls, intrusion prevention or detection systems, anti malware (ad-aware, spyware, virus, worm, etc.) software and other.

BACKGROUND

Security and Behavioral Aspects

Information security is not only about infrastructure, software or networks (Aytes & Connolly, 2003; Rhee, Kim, & Ryu, 2009; Ng & Rahim, 2005; Ng & Xu, 2007; Workman, Bommer, & Straub, 2008). Users and their attitudes are of equal importance (Herath & Rao, 2009; Rhee et al., 2009; Stanton et al., 2005) since they play a dominant role at the implementation of information security policies and countermeasures. If *human factors* are neglected, information security issues are restricted into a technical perspective which is not realistic and may end up in erroneous conclusions regarding the *information security readiness* within organizations, institutions or any other kind of user communities. Inline with this ascertainment, a series of research works identify the importance of end-users attitudes, beliefs and behaviors in implementing effective information security (Aytes & Connolly, 2003; Herath & Rao, 2009; Ng & Rahim, 2005; Ng & Xu, 2007; Stanton et al., 2005; Workman et al., 2008; Yeo, Rahim, & Ren, 2008).

Research on *information security behavior* is still in its infancy and researchers urge to identify pathways towards in-depth investigation of behavior in regards to information security (Stanton et al., 2005, p. 125). Several attempts may be identified in the literature, which empirically adapt theories and assess dimensions from a variety of scientific domains, mainly emphasizing on constructs from